REMARKS

In section 1 of the Office Action, the Examiner objected to claim 30 as being a substantial duplicate of claim 29. Accordingly, claim 30 has been canceled.

In section 2 of the Office Action, the Examiner objected to claim 32 as being a substantial duplicate of claim 31. Accordingly, claim 32 has been canceled.

In section 3 of the Office Action, the Examiner rejected claims 31 and 32 under 35 U.S.C. §101 as being directed to non-statutory subject matter.

Claims 31 has been amended to overcome the rejection.

As indicated above, claim 32 has been canceled.

In section 5 of the Office Action, the Examiner rejected claims 17, 18, and 27-32 under 35 U.S.C. §102(e) as being anticipated by McCallam '832.

McCallam '832 describes a recovery architecture 300 that is stored in a ROM 208 of a security server 114. The security server 114 includes a processor 204 that recovers information compromised by an information warfare (IW) attack.

The recovery architecture 300 includes a recovery manager 370 and an agent manager 320. The agent manager

320 uses software agents 321 to collect information from the network. The collected information is processed and stored in a database 330 and is used to restore the network to full operational status.

The recovery manager 370 directs execution of information warfare attack recovery routines. A detection manager 375 of the recovery manager 370 detects possible intrusion or misuse. A recovery system 393 of the recovery manager 370 implements the recovery routines. The recovery system 393 includes a damage assessment module 401 and recovery routines 402. The recovery routines 402 include primary reconstitution routines 403 and secondary reconstitution routines 404.

The damage assessment module 401 determines the extent of data corruption and other damage that may have occurred to the network devices 101 by executing check sum operations on selected data.

The detection manager 375 detects an information warfare attack in the network. The detection manager 375 includes a comparator 377 and a data storage device 379. The comparator 377 examines data such as computer performance parameters 410 collected by the software agents 321 and compares the data to a predefined condition. If

the comparison indicates a possible information warfare attack, the detection manager 375 provides an alert.

More particularly, the comparator 377 compares the collected parameters 410 to a user profile 400 that reflects normal operation of the network device 101. If the comparison indicates an unusual behavior pattern, the detection manager 375 generates the alert. The parameters 410 may exceed the user profile 400, or a trend of the performance parameters 410 may indicate that a limit will soon be exceeded, or a combination of specific performance parameters 410 may indicate a potential information warfare attack. The comparator 377 includes logic 369 to analyze the relationship between the performance parameters 410 to determine if they indicate a specific type of problem.

For example, a comparison of the parameters 410 to the user profile 400 may indicate excessive disk access with many read/write operations. If a high number of erasures is also detected, a purging of a computer memory may be inferred. Such purging may in turn indicate computer misuse or intrusion.

When implemented on the security server 114, the comparator 377 compares the computer performance parameters 410 to a network version of the user profile 400, and the

comparator 377 in addition compares a local version of the user profile 400 to the network version of the user profile 410. A divergence between the network version and the local version may indicate tampering with the network device in an attempt to mask an information warfare attack.

The process of preparing for, responding to, and recovering from an information warfare attack includes a pre-information warfare attack routine 500, an information warfare attack response routine 600, and a network recovery routine 500. The pre-information warfare attack routine 500 determines what information is needed for recovery. The information warfare attack response routine 600 assesses damage from the information warfare attack, takes corrective actions, and selects appropriate recovery routines. The network recovery routine 700 retrieves the recovery information, restores information to damaged areas of the network, and restores the network to full operational status.

Independent claim 17 - As can be see from the description above, McCallam '832 does not compare instruction data with a first profile when the instruction data is received while the computer is not logged into a user account and with a second profile when the instruction

data is received while the computer is logged into a user account. Not only does McCallam '832 simply not make the distinction between when a user is logged in and when no user is logged in, but it can be easily inferred from McCallam '832 that all monitoring is done while users are logged in.

Accordingly, independent claim 17 is not anticipated by McCallam '832.

Because independent claim 17 is not anticipated by McCallam '832, dependent claims 18 and 27, and 28 likewise are not anticipated by McCallam '832.

Independent claim 29 - McCallam '832 does not disclose the use of a profile that includes operations not identified with specific users and a profile that includes only operations identified with specific users. McCallam '832 describes only user profiles, which necessarily includes only operations identified with specific users.

Moreover, as discussed above, McCallam '832 does not compare instruction data with a first profile when the instruction data is received while the computer is not logged into a user account and with a second profile when the instruction data is received while the computer is logged into a user account. Not only does McCallam '832

simply not make the distinction between when a user is logged in and when no user is logged in, but it can be easily inferred from McCallam '832 that all monitoring is done while users are logged in.

Accordingly, independent claim 29 is not anticipated by McCallam '832.

Because independent claim 29 is not anticipated by McCallam '832, dependent claims 33-35 likewise are not anticipated by McCallam '832.

Independent claim 31 - McCallam '832 does not disclose the use of a profile that includes a power on operation of a computer.

Moreover, as discussed above, McCallam '832 does not compare instruction data with a first profile when the instruction data is received while the computer is not logged into a user account and with a second profile when the instruction data is received while the computer is logged into a user account. Not only does McCallam '832 simply not make the distinction between when a user is logged in and when no user is logged in, but it can be easily inferred from McCallam '832 that all monitoring is done while users are logged in.

Accordingly, independent claim 31 is not anticipated by McCallam '832.

Because independent claim 31 is not anticipated by McCallam '832, dependent claims 36-38 likewise are not anticipated by McCallam '832.

In section 7 of the Office Action, the Examiner rejected claims 19-26 under 35 U.S.C. §103(a) as being unpatentable over McCallam '832 in view of McCallam '834.

McCallam '834 fails to make up for the deficiencies of McCallam '832. Therefore, independent claim 17 is patentable over McCallam '832 in view of McCallam '834. Because independent claim 17 is patentable over McCallam '832 in view of McCallam '834, dependent claims 19-26 are *per force* patentable over McCallam '832 in view of McCallam '834.

CONCLUSION

In view of the above, the claims of the present application patentably distinguish over the art applied by the Examiner. Accordingly, allowance of these claims and issuance of the present application are respectfully requested.

The Commissioner is hereby authorized to charge any additional fees that may be required, or to credit any overpayment, to account No. 501519.

Respectfully submitted,

SCHIFF HARDIN LLP
6600 Sears Tower
233 South Wacker Drive
Chicago, Illinois 60606-6402
(312) 258-5774
CUSTOMER NO. 26574

By: _____
Trevor B. Jolke
Reg. No: 25,542

January 16, 2009